~~FOR OFFICIAL USE ONLY~~

November 30, 2005

Information Technology Management

Report on Diagnostic Testing at the Defense Information Systems Agency, Center for Computing Services (D-2006-030)

~~SPECIAL WARNING~~

~~This report contains information exempt from mandatory disclosure under the Freedom of Information Act, Exemption 2.~~

Department of Defense
Office of Inspector General

Constitution of the United States

A Regular Statement of Account of the Receipts and Expenditures of all public Money shall be published from time to time.

Article I, Section 9

~~FOR OFFICIAL USE ONLY~~

Additional Copies

To obtain additional copies of this report, contact the Secondary Reports Distribution Unit, Audit Followup and Technical Support at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact Audit Followup and Technical Support at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

ODIG-AUD (ATTN: AFTS Audit Suggestions)
Department of Defense Inspector General
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704

Acronyms

DISA	Defense Information Systems Agency
CS	Center for Computing Services
FSO	Field Security Operations
HIDS	Host-based Intrusion Detection System
IAO	Information Assurance Officer
MIAG	Mandatory Information Assurance Guidance
SA	System Administrator
SDID	Short Description Identifier
SNMP	Simple Network Management Protocol
SSH	Secure Shell
STIG	Security Technical Implementation Guide
VMS	Vulnerability Management System

November 30, 2005

MEMORANDUM FOR DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

SUBJECT: Report on Diagnostic Testing at the Defense Information Systems Agency, Center for Computing Services (Report No. D-2006-030)

We are providing this report for information and use. We considered management comments on a draft of this report in preparing the final report.

Comments on the draft of this report conformed to the requirements of DoD Directive 7650.3 and left no unresolved issues. Therefore, no additional comments are required.

We appreciate the courtesies extended to the staff. Questions should be directed to [redacted] at (703) 325-[redacted] (DSN 221-[redacted]) or [redacted] at (703) 428-[redacted] (DSN 328-[redacted]). For the report distribution, see Appendix E. The team members are listed inside the back cover.

By direction of the Deputy Inspector General for Auditing:

Paul J. Granetto, CPA
Assistant Inspector General
Defense Financial Auditing Service

(Report No. D-2006-030) **November 30, 2005**
(Project No. D2004-D000FG-0191.002)

MEMORANDUM FOR DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

SUBJECT: Report on Diagnostic Testing at the Defense Information Systems Agency, Center for Computing Services

Who Should Read This Report and Why? Department of Defense (DoD) personnel who use the services provided by Defense Information Systems Agency (DISA), Center for Computing Services (CS) may find this report of interest, as will other CS user organizations. Persons who supervise any part of the DoD information assurance program may also find this report useful. This is one of three technical reports in support of the overall Statement on Auditing Standards No. 70 report on Defense Information Systems Agency, Center for Computing Services. This report will describe the results of diagnostic testing over the technical controls on selected assets in the CS environment.

Background. The CS provides computer processing for the entire gamut of combat support functions, including transportation, logistics, maintenance, munitions, engineering, acquisition, finance, medicine and military personnel readiness. With more than 800,000 users, CS operates over 1,400 applications utilizing more than 40 mainframes and 3,275 servers. The reliability of the general controls directly impacts the individual finance and accounting systems, any of the feeder systems, and ultimately DoD's ability to produce reliable and auditable financial statements, as required by the Chief Financial Officer's Act of 1990 (P.L. 101-576). The general controls testing encompass diagnostic testing; the testing of the technical controls implemented in the CS environment.

Criteria. DoD Directive 8500.1, "Information Assurance," November 21, 2003, requires that all information assurance and information assurance-enabled information technology products incorporated into DoD information systems shall be configured in accordance with DoD-approved security configuration guidelines. DISA Field Security Operations (FSO) develops guidelines, referred to as Security Technical Implementation Guides (STIGs). The STIGs assist in securing CS systems against security and infrastructure vulnerabilities.

The STIGs were used as the primary criteria during diagnostic testing. For complete list of STIGs and Security Checklists (Checklists) used as the testing criteria, see Appendix C. Compliance with the applicable STIGs was mandatory for systems residing in a CS facility and for any system directly administered by CS. Use of STIGs provides an environment that meets or exceeds the security requirements of DoD systems operating at the Mission Assurance Category II Sensitive level. In addition, to connect any asset to a CS network, the asset must comply with the Mandatory Information Assurance Guidance (MIAG) policy letter 05-1, May 1, 2005. This policy letter provides the allowable level of acceptable open vulnerabilities to operate in the environment, and we used this criterion to determine the individual asset's pass or fail conclusion. We developed diagnostic testing audit programs (also referred to as work programs) using the STIG criteria to identify vulnerability severity code (i.e. Category I) for each testing procedure. DISA defined Category I as any vulnerability that may result in a total loss of information and that provides an unauthorized person or software immediate access into a system, gains privileged access, bypasses a firewall, or results in a denial of service.

DISA defined Category II as any vulnerability that provides information that has a high potential of giving access to an unauthorized person, or provides an unauthorized person the means to circumvent security controls. Different STIGs refer to the specific vulnerabilities with a code number and a short name: UNIX and mainframe STIGs use Short Description Identifiers (SDIDs), Windows STIGs use Potential Discrepancy Items, and Network STIGs use NETs. This report only uses SDIDs for all vulnerability types to simplify vulnerability terminology for the reader. Specific technical terms used in this report are defined in Appendix D.

Objectives. The overall audit objective was to evaluate whether CS implemented controls to ensure that its systems and processes were secure and complied with significant applicable guidance. Specifically, our audit is to determine whether CS: (1) general and application controls were adequately designed and effectively operating; (2) complied with the Federal Financial Management Improvement Act and other applicable laws and regulations; and (3) properly certified and accredited its computing environment in accordance with the Department of Defense Information Technology Security Certification and Accreditation Process.

This report contains the results from the diagnostic testing in support of the objective to determine the adequacy of general controls. Another report, General and Application Controls at the Defense Information Systems Agency, Center for Computing Services, will cover all three stated objectives. See Appendix A for a detailed discussion of the scope and methodology.

Results. The information obtained from the diagnostic testing identified a number of exceptions to the published STIG requirements. Based on the MIAG, 3 of 5 Client and Server, 3 of 7 IBM mainframes, 6 of 27 network devices, 41 of 49 UNIX devices, and 36 of 54 Windows devices failed the criteria for each respective type of devices[1]. We identified exceptions for Tandem systems and Unisys devices; however, the number and severity of the exceptions did not exceed the allowable thresholds defined in the MIAG. Details of the sampling approach can be found in Appendix B. Specifically, CS diagnostic testing had exceptions to technical controls in the following areas:

- permissions, settings, and services (finding A);
- automated scripts (finding B);
- password policies (finding C);
- account maintenance (finding D);
- intrusion detection (finding E);
- system patches (finding F);
- system file baselines (finding G);
- encryption (finding H); and
- outdated technologies (finding I).

[1] The numbers of systems only apply to the total items tested, and not the decommissioned items discovered during field testing. The number for IBM mainframes includes items tested in Group B and Group I. See Appendix B for more detail.

Management Comments and Audit Response. DISA CS response for the Director, Center for Computing Services, and Chief, Field Security Operations, concurred with all 19 recommendations. See the individual findings for a discussion of management comments and the Management Comments section of the report for the complete text of the comments.

Finding A. Permissions, Settings, and Services. Compliance of technical controls with DoD and CS requirements and guidance needed improvement.

- Permissions to limit access to devices, directories and files, and registry setting, were not in compliance with DoD and DISA policies.
- Configuration and security settings for network, UNIX, Windows, and mainframe devices, were not in compliance with DoD and DISA guidelines.
- Services running on devices, configured incorrectly or should have been disabled, were not in compliance with DoD and DISA guidelines.

As a result, vulnerabilities created from incorrectly set permissions and settings could compromise the device and provide users with unauthorized access to configuration settings and data. In addition, running unnecessary services could expose the network to the vulnerabilities inherent in those services. Malicious users could attack the services and further exploit the network or systems.

Permissions to Limit Access. Permissions to limit access to devices, directories and files, and registry settings, were not in compliance with DoD and DISA policies. Specifically, assets had incorrectly set permissions that allowed access to directories and files and the ability to change system settings, registry keys, and policies. As a result, sensitive information on a device, such as configuration settings and data, could have been compromised by unauthorized users. The examples included below demonstrate the non-compliant permission settings to limit access for User File Creation Mode Mask (umask) and file permissions, IBM mainframe, Tandem, and Windows registry.

Umask and File Permissions. The system administrators (SAs) did not configure 25 of 49 UNIX umask settings to 077. Umask defines permissions a file has when the file is initially created on the UNIX device. Umask is a function that sets the default file system permissions for newly created files. The UNIX STIG (SDID G089) requires that the Umask be set to a default value of 077, so only the file owner has read, write, and execute privileges while other users have no privileges.

The incorrect umask setting has a direct impact on file permission compliance. Configurations on 24 of 49 UNIX devices had more permissive access settings than allowed by the STIGs and did not have documentation justifying the business need. The UNIX STIG (SDID G053) requires the SA to ensure user home directories have initial access permissions set to 700, and never more permissive than 750 unless fully justified and documented by the Information Assurance Officer (IAO). A directory with permission of 700 allows read, write, and execute privileges to the owner and no privileges to user's group or any other users. A directory with permissions of 750 allows read, write, and execute privileges to the owner; read and execute privileges to the user's group; and no privileges to any other users. Incorrect umask settings could allow users unauthorized access to data and settings on UNIX devices.

IBM Mainframe Permissions. The SAs incorrectly configured access rights to sensitive data set or system command access for seven of seven IBM mainframe devices. The operator commands allow users to alter execution parameters, terminate processes, perform system shutdowns, and; therefore, endanger system integrity and stability. The OS/390 STIG (Sections 2.1.2.1, 2.1.2.10, 3.1.2.1, 3.1.5.6, 3.2.1, 3.2.4.4, and 3.4.4.4) defined the required user access, data set and authorized program facility protection, and system command protection settings.

Tandem Permissions. The SAs incorrectly configured access rights and permissions on all three Tandem devices. For example, for one of the three Tandem systems, sensitive system files (TACLLOCL files) had access permissions that allowed anyone to access the files. Tandem Advanced Command Language is used to access the system administration utilities and access to the global startup files presents opportunities for system penetration or disruption. The Tandem STIG (Sections 4.2.1.1, 4.2.2, and 5.6) defines the required user and administrator group access and data set (sensitive files) protection settings.

Windows Registry Permissions. The SAs incorrectly set user rights assignments for 25 of 54 Windows devices. User rights define the user's ability to perform certain system functionality, for example, the ability to log on as a batch job. The Windows 2000 Checklist (SDID 4.010) and Windows NT Checklist (SDID 4.010) define the list of required user rights assignments and the type of accounts with the associated rights assignments. For example, no generic user account should be able to log on as a batch job. With these permissions set incorrectly, generic users could perform system level functions that could potentially elevate their privileges on the Windows systems.

Configuration and Security Settings. Configuration and security settings were not in compliance with DoD and DISA guidelines for network, UNIX, Windows, and mainframe devices. SAs incorrectly configured security settings, such as account lockout settings; mainframe settings to key system resources, files, and data; settings to registry keys and broadcast settings; and security warning banner display. Configuration and security settings that do not comply with the STIGs could expose the CS production environment to vulnerabilities from within the device, as well as from external malicious users. The examples below demonstrate the incorrect configuration and security settings for account lockout settings, IBM mainframe settings, Tandem settings, registry keys, broadcast presence on network setting, and warning banners.

Account Lockout Settings. The SAs incorrectly configured account lockout settings for 21 of 49 UNIX devices. The UNIX STIG (Section 3.1.3) requires the device be configured to only allow failed logons with an interval of at least two seconds between logon attempts and to lock the account after three failed attempts. The UNIX STIG also requires accounts be locked until the IAO or the system unlocks the account after a minimum of 30-minute delay. For any accounts that are locked, the IAO must review the circumstances causing locked accounts to ensure there are no security concerns. Incorrect account lockout settings could allow a malicious user to discover a username and password combination through a continuous attack on a device.

IBM Mainframe Settings. The SAs incorrectly configured seven of seven IBM mainframe devices had system security software settings relating to sensitive libraries, data sets, or started procedures. The OS/390 STIG (Sections 3.1.5.1, 3.3.2.3, 3.3.4.1,

3.3.4.3 and 3.3.5.1) defines the standards for security settings of sensitive libraries, datasets, and started procedures. Examples included a dataset containing userids and passwords with a default access of read, and multiple Authorized Program Facility libraries not defined for protection. The Authorized Program Facility specifies programs allowed to use sensitive system functions, access to Authorized Program Facility libraries creates the potential for an unauthorized program to access audit logs and other data by circumventing access control software. Improper configuration of the operating system could result in unauthorized access to CS resources.

Tandem Settings. The SAs incorrectly configured system security settings on all three Tandem devices. The Tandem STIG (Sections 4.2.5, 4.2.2, 5.6, and 4.2.1.1) defines default subvolume protection requirements. For example, the default system subvolumes located on the Tandem $SYSTEM volume were not set in compliance with the STIG. Some default subvolumes contained several system utilities reference files; therefore, unauthorized access to these subvolumes and modification of associated contents could negatively impact the functioning of utility programs. Improper configuration of the operating system could result in unauthorized access to CS resources. Furthermore, the capabilities of the utility programs could be leveraged to obtain unauthorized access to other system resources.

Registry Keys. The SAs incorrectly configured 14 of 54 Windows devices that allowed non-administrators to change settings contained in the registry files. Registry keys maintain the Windows operating system configuration information. The Windows 2000 Checklist **(**SDID 3.009) requires the SA to ensure that non-administrators cannot change the command associations for registry files. Access to the registry and registry key by a non-administrator could compromise the system. As a result, the system could be prone to system outages or crashes because of incorrect registry settings.

Broadcast Presence on Network Setting. The SAs incorrectly configured 8 of 54 Windows devices announced themselves to domain master browsers because of an incorrect setting. A domain master browser is used to collect and maintain a list of all available servers on a network. The Windows 2000 Checklist (SDID 5.085) requires the SA to enable the option "*hide computer name from other domain computers*" to prevent servers from announcing their presence on the network. Incorrectly setting this option provides a list of Windows devices present on the network that a malicious user could potentially exploit.

Warning Banners. The SAs did not deploy warning banners on 9 of 32 network devices[2]. The Network Checklist (SDID 0340) requires that the Network Security Officer to ensure deployment of warning banners on all network devices allowing Secure Shell (SSH), telnet, file transfer protocol, or hypertext transfer protocol access in accordance with DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003.

Services. Services running on devices were not in compliance with DoD and DISA guidelines. Specifically, services were either configured incorrectly, should have been disabled, or missing justification and documentation. Services enabled on a device listen for requests and send requests on the network. These requests could be legitimate or

[2] We combined client server and network devices because these devices follow the Network STIG and for reporting purposes.

malicious. Running unnecessary services, or services not properly secured, could introduce vulnerabilities to the device if malicious users are able to make requests to the device. As a result, a malicious user could exploit vulnerabilities of the service to gain access to the device. Therefore, all unnecessary services should be disabled or shutdown. The following examples demonstrate the non-compliant services for UNIX network services; simple network management protocol (SNMP); telnet; sendmail; and cron services.

UNIX Network Services. The SAs did not disable unnecessary services on 42 of 49 UNIX devices. The UNIX STIG (Section 4) requires the SA to disable the non-exhaustive list of potential network services not usually necessary for operations unless justified and documented with the Information Assurance Manager and IAO. For example, the systems running telnet, file transfer protocol, and other network services could listen for requests on the network and could expose the device to outside attacks.

Simple Network Management Protocol. The SAs did not implement SNMP version 3 on 9 of 32 network devices. The network STIG (SDID 1660) requires that the SNMP version 3 security model be used across the entire network infrastructure to prevent unauthorized access. Devices not running SNMP version 3 send and receive commands and log data across the network in plain text that could be intercepted by eavesdropping on the network. Data and commands intercepted could be used to compromise the device.

Telnet. The SAs deployed or incorrectly configured telnet on 11 of 54 Windows devices. These 11 Windows devices also lacked the required justification and documentation. The telnet application is used to provide text-based login sessions between two computers on a network. The Windows 2000 Checklist (SDID 5.013) requires the IAO to ensure that sites do not deploy a Windows NT and Windows 2000-based telnet server. Telnet passes usernames and passwords across the network in clear text and could result in a user account compromise.

Sendmail. The SAs implemented outdated versions of sendmail on 8 of 49 UNIX systems. Sendmail is a computer program that is used for the routing and delivery of email. The UNIX STIG (SDID V124) requires the SA to ensure that the latest version of sendmail is implemented. The older version of sendmail could be used to send spam or malicious emails.

Cron Service. The SAs incorrectly configured or did not configure the cron.deny and cron.allow files for 20 of 49 UNIX devices. The cron service, a task manager for UNIX systems, is used to schedule commands to be executed periodically. The cron.deny and cron.allow files are used as access controls to limit user access to the cron service. The UNIX STIG (SDID 200) requires the SA to control access to the cron utilities via the cron.allow or the cron.deny file. If cron is not limited to authorized users, malicious users can change scheduled cron jobs or malicious users could use cron to schedule malicious activities.

Incorrectly configured permissions, settings, and services existed across all platforms tested. The number of incorrect settings and exceptions to the STIGs, as well as other issues identified in this report, indicated a need to improve SA training. The SAs need more education on the specific SDIDs that they must follow to secure the system and the

manual tests that must be performed to supplement to the automated scripts. The SA training should also include adopting the Joint System Administration checklist that outlines the periodic tasks an SA should perform.

Recommendations A.

A.1. We recommend that the Director, Center for Computing Services, develop a program to familiarize the system administrators of their specific roles in determining compliance. This program should include the following:

A.1.a. Specific Security Technical Implementation Guide Short Description Identifiers that the system administrators must comply with.

Management Comments. The Director concurred and stated that his office has a System Administrator Certification Program in place and the FSO has developed a plan to take over the responsibility of the Program. The Director further stated that his office would complete the Systems Administrator Certification for current SAs requiring further training by December 31, 2005.

A.1.b. Specific guidance on how to manually test Security Technical Implementation Guide Short Description Identifiers not tested by the automated scripts.

Management Comments. The Director concurred and stated that the System Administrator Certification Program covers instructions on how to manually test Security Technical Implementation Guide Short Description Identifiers not tested by the automated scripts. CS would complete the Systems Administrator Certification for current SAs requiring further training by December 31, 2005.

A.2. We recommend that the Director, Center for Computing Services, require the implementation of the Joint System Administration Checklist, May 25, 2005, or an equivalent, that provides system administrators with a list of tasks to be performed to bring the devices they manage into compliance with the Windows, UNIX, Tandem, IBM (OS/390), and Network Security Technical Implementation Guides.

Management Comments. The Director concurred and stated that the Joint System Administration Checklist had been incorporated at all CS sites.

A.3. We recommend that the Director, Center for Computing Services, enforce the compliance with the Security Technical Implementation Guides for access permission settings, configuration and security settings, and disabling of unnecessary services.

Management Comments. The Director concurred and stated that all site Information Assurance Managers have been re-briefed on the Security Technical Implementation Guides requirements to include access permissions settings and configuration and security settings. CS would complete Systems Administrators Certification for current SAs requiring further training by December 31, 2005.

Finding B. Automated Scripts. The automated UNIX script did not accurately report STIG compliance exceptions. The SAs who managed the devices depended on the automated script to identify exceptions that are not in compliance with STIG requirements. Specifically, the script did not check for all daemons, which are services on a UNIX system, or verify that only authorized shells were listed in the /etc/shells file. When the automated scripts did not report that a particular security setting had not met STIG requirements, or when the automated scripts did not identify the condition as an exception, then the exception or deficiency would not be identified by the SA and the system would remain non-compliant.

The process for checking compliance included executing the automated scripts on a weekly basis. The SAs examined the output from the automated scripts for any "Open" item, or exceptions, reported by the automated scripts and attempted to fix it as soon as possible. If the automated scripts did not list any "Open" items, the SA would not perform additional checks; they depended on the automated scripts to identify noncompliant system security settings.

Daemons. A daemon (analogous to a service in Windows) is a computer program that runs in the background, rather than under the direct control of a user. The UNIX STIG (SDID G036) requires that daemons have permissions of 755[3], or more restrictive. The automated script used during the testing period to test this requirement searches from a list of 28 daemons; however, the list incompletely identified the daemons in the most recent operating system version. Without checking for all possible daemons, the risk is increased that a malicious program can be substituted for the daemon.

Authorized Shells. The automated scripts did not check for shells authorized by the IAO. The UNIX STIG (SDID G069) specified that the SAs enter all authorized shells in the /etc/shells file. One UNIX device had unauthorized shells in the /etc/shells file, and the automated scripts did not report this as a finding. The SA commented he was unaware of those shells present in the /etc/shells file and; therefore, had not received authorization for those shells.

To test for compliance to the UNIX STIG (SDID G069), the automated script executed the following steps:

- Added header information to the report
- Set the default answer of the test to "Answer=2" (not a finding)
- For operating systems that are not AIX, the script checked for the presence of the /etc/shells file. If the file is present, then it reported "Not a Finding," and did not review the contents of the file or check against authorized shells.

For each of the script results reviewed, the script set the default result to "Answer=2" or "Not a Finding." However, if the script did not find all of the information necessary to test for compliance to the STIG, or if the device did not meet all of the tests for compliance, then the result defaulted in "Not a Finding."

[3] A permission of 755 indicates that the daemon will have restricted access of read, write, and execute for the daemon owner, and read and execute access to any other user with access to the system.

Since testing of this specific STIG requirement with the automated script resulted with a default "Not a Finding," some devices incorrectly passed this test. As a result, some devices can be incorrectly identified as meeting the STIG requirements but have findings that were not identified by the automated scripts.

The SAs relied on these automated scripts to identify and correct areas of STIG non-compliance. If the results identify an "Open" item after running the automated scripts, then SAs take appropriate corrective action. Because the results of running the automated scripts could report a false passing of the individual STIG requirement, the SAs may not be aware that they need to take corrective action. This increases the risk that devices deployed in the production environment with non-compliant configurations could inadvertently be compromised by a malicious user.

As a planned improvement to the automated script and reporting process, the next release of Vulnerability Management System (VMS) will require the preparation of a Plan of Action and Milestone for situations that require time to develop and apply a correction or fix. Additionally, the next release of VMS will support the capability to load self-assessments directly into the database, thus providing accountability for each review action. An interface with the System Support Office Montgomery Automated Tool Kit (automated scripts) is also being developed. This interface will load the results of the Tool Kit directly into VMS, providing a more timely and accurate picture of the overall information assurance posture of each system at the data centers.

Recommendations B.

Revised Recommendation. As a result of management comments, we revised draft Recommendation B.1. to direct the Chief, Field Security Operations to only review the current scripts to ensure compliance with the Security Technical Implementation Guide for UNIX.

> **B.1. We recommend that the Chief, Field Security Operations review the current scripts to determine if the information collected from the scripts provide enough assurance on the compliance or non-compliance of the device with the Security Technical Implementation Guide for UNIX requirements.**

Management Comments. The Chief, FSO, concurred and stated that his office will update the UNIX scripts by first quarter CY 2006 to accurately check for all possible daemons or services. Additionally, FSO has added a contract modification to add Security Technical Implementation Guide compliance testing and policies to scanning and reporting tools. The projected completion date is December 31, 2006.

> **B.2. We recommend that the Chief, Field Security Operations change the default value for the automated scripts from "Not a Finding" to "Not Reviewed" or some indicator that the script did not fully execute the test for compliance.**

Management Comments. The Chief, FSO, concurred and stated that the script fix actions would be completed in phases. The Chief stated that approximately 10 percent of the scripts were corrected in July 2005. The projected completion for all affected UNIX

scripts is April 2006. Additionally, FSO has added a contract modification to add Security Technical Implementation Guide compliance testing and policies to scanning and reporting tools. The projected completion date is December 31, 2006.

B.3. We recommend that the Director, Center for Computing Services, develop manual procedures for items reported by the automated script as "Open" and "Not Reviewed" and enforce performance of these procedures by the system administrators.

Management Comments. The Director concurred and stated that CS requires manual checks of all items reported by the automated script as "open" or "not reviewed" and enforces compliance with manual procedures already in place. The Director stated that the FSO is in the process of updating the SRR scripts and expects to complete the SRR scripts by CY 2006. The SSO is also in the process of developing a Gold Disk for UNIX operating systems that will correct this finding.

Finding C. Password Policies. Password configurations did not always comply with DoD and DISA guidelines. For example, some password lengths were shorter than the minimum requirement, and some password aging (the length of time a password can be used) was longer than the maximum time period allowed. As a result, the SAs did not find and remove noncompliant passwords or passwords did not expire for an extended period of time.

DoD Instruction 8500.2 requires that passwords be set at a minimum, to include a case sensitive, 8-character mix of upper case letters, lower case letters, numbers, and special characters, including at least one of each (e.g., emPagd2!). At least four characters must be changed when creating a new password. The DISA Handbook requires that the password be changed every 90 days. Additionally, the UNIX STIG (SDID L112) requires the SA to execute one of the password cracking tools weekly and send the results to the IAO. Finally, the Windows Checklist (SDID 3.057) requires disabling password decryption. Devices below did not comply with DoD and DISA password policies.

- Sixteen of 49 UNIX devices did not have a password cracking tool run on a weekly basis.
- Eighteen of 54 Windows devices did not have the password expiration set for the administrator account.
- Six of seven IBM mainframe logical partitions did not have the correct setting for password change interval or minimum password length.
- Three of three Tandem devices did not check password complexity.
- One of 7 Unisys mainframes had incorrect setting for password expiration.
- Six of 54 Windows devices did not set the registry key to prevent the reversible encryption of stored passwords.

Shorter password lengths and infrequently changed passwords increase the likelihood of a successful brute force attack against the account. The use of the CS mandated password cracking tool helps identifying easy-to-guess passwords.

Recommendations C.

> **C.1. We recommend that the Director, Center for Computing Services, enforce compliance with the Security Technical Implementation Guides and ensure that password cracking tools are run on a weekly basis.**

Management Comments. The Director concurred and stated that CS runs password-cracking tools on a weekly basis on all systems. The Director further stated that the System Administrator Certification Program addresses DoD and DISA password requirements. The Director would complete the Systems Administrator Certification for current SAs requiring further training by December 31, 2005.

> **C.2. We recommend that the Director, Center for Computing Services, enforce Department of Defense policy that requires passwords to be set, at a minimum, with a case sensitive, 8-character mix of upper case letters, lower case letters, numbers, and special characters, including at least one of each, and that passwords are changed every 90 days.**

Management Comments. The Director concurred and stated that the System Administrator Certification Program addresses DoD and DISA password requirements and that CS would complete the System Administrator Certification for current SAs requiring further training by December 31, 2005.

> **C.3. We recommend that the Director, Center for Computing Services, identify all customer applications that do not comply with system level password required settings, assess the risk presented by each instance of non-compliance, and require changes to the application or operating system to modify them to comply with the password requirements where the risks presented are unacceptable.**

Management Comments. The Director concurred and agreed to work with customers to implement changes to their applications that are needed to meet the minimum user name and password requirements. Local site Directors are working with the customers to gain support and cooperation in enforcing compliance with the required password settings.

> **C.4. We recommend that the Director, Center for Computing Services, check for and confirm registry keys that pertain to reversible password encryption are set to Department of Defense and Defense Information Systems Agency guidelines.**

Management Comments. The Director concurred and stated that CS checks for and confirms that registry keys pertaining to reversible password encryption settings are set to comply with DoD and DISA at all sites and locations. The Director further stated that all sites were in compliance as of October 17, 2005.

Finding D. Account Maintenance. SAs did not implement account maintenance practices and procedures correctly for all devices. Specifically:

- SAs did not disable or change default accounts and passwords.
- SAs did not disable or delete inactive user accounts on systems after a period of non-use.

As a result, the affected devices introduced security weaknesses into the environment that could introduce or propagate unauthorized or unintended access. Malicious users could use inactive or dormant accounts to access systems and modify sensitive data. Furthermore, since inactive accounts get recognized as legitimate accounts within the networking environment, malicious activities may be undetected.

Default Accounts. SAs did not disable default accounts. Default accounts are accounts created when the operating system is installed or applications are installed on a device. Default accounts are well-known and present a target for exploitation. As a result, devices with well-known default account and passwords may be compromised with little effort.

- SAs did not disable default accounts on 4 of 49 UNIX devices by setting the shell to /bin/false, /usr/bin/false, /sbin/false, or /dev/null, as required by the UNIX STIG (SDID G092).
- SAs did not rename or disable default accounts on 23 of 54 Windows NT and Windows 2000 devices, as required by the Windows Checklist (SDIDs 4.022, 4.021, and 4.020).

Inactive Accounts. The SAs did not deactivate or delete inactive accounts beyond the allowed time limits on 28 of 49 UNIX devices. The UNIX STIG (section 3.1) requires that accounts not used in over 35 days be locked out, and then deleted after a period of 90 days of inactivity.

Recommendations D.

D.1. We recommend that the Director, Center for Computing Services, enforce the disabling of default accounts.

Management Comments. The Director concurred and stated that CS would reiterate the DoD and DISA guidelines for enforcing the disabling of default accounts at all sites and locations to the Directors and Deputy Directors during the CS Operations Conference from October 31, 2005 to November 4, 2005.

D.2. We recommend that the Director, Center for Computing Services, enforce the disabling of user accounts after a period of non-use and deletion of inactive user accounts.

Management Comments. The Director concurred and agreed to enforce the DoD and DISA guidelines for disabling user accounts after a period of non-use and deleting inactive accounts. Additionally, the Director stated that all departing employees' accounts are deleted or reassigned with a new user account name and password during the check out process. The Director further stated that the System Administrator Certification Program addresses DoD and DISA password requirements and that CS would complete the Systems Administrator Certification for current SAs requiring further training by December 31, 2005.

Finding E. Intrusion Detection. CS did not deploy host-based intrusion detection system (HIDS) software on 30 of 54 Windows servers. DoD Instruction 8500.2 requires that HIDS be deployed for all major applications and for network management assets such as routers, switches, and domain name servers. In addition, the Windows STIG (SDID 1.025) requires the Information Assurance Manager to ensure DoD servers use HIDS.

Intrusion attempts and successes may go unnoticed on the devices without HIDS. CS administrators may have difficulty detecting, preventing, and responding to attacks designed for operating systems. Specifically, attempts to obtain privileged access by exploiting vulnerabilities may go undetected. Once a system is compromised, attempts to compromise other systems may blend in with "normal" network traffic and go unnoticed. Additionally, operating multiple production systems without a HIDS may give CS information security professionals an incomplete picture of their network security.

According to CS personnel, DoD plans to purchase an enterprise license for HIDS in the near future. CS made a risk management decision to only purchase HIDS for critical systems and await the DoD purchase for mass implementation. However, in the interim, this represents a control risk.

Recommendation E.

> **E.1 We recommend that the Director, Center for Computing Services, identify all assets without host-based intrusion detection systems and implement host-based intrusion detection system as required by Department of Defense and Defense Information Systems Agency policies.**

Management Comments. The Director concurred and stated that CS will implement HIDS enterprise wide once the DoD IA Work Group publishes guidance.

Finding F. System Patches. SAs did not always implement critical updates and system software patches for UNIX and Windows systems, or did not document that the customer waived the requirement to patch the systems. SAs may have misunderstood who authorized updates and system software patches, and the patch installation process. Running devices not adequately patched could introduce vulnerabilities already widely known, and a malicious individual could exploit the vulnerability. A patch release mitigates vulnerabilities, and the patch documentation also describes the vulnerability. The devices without patches posed risks to the CS network environment. Patching devices mitigates a substantial number of known vulnerabilities.

- SAs did not apply required software patches to 44 of 49 UNIX devices. The UNIX STIG (SDID G033) requires that the SA ensure required software

patches are applied to all devices and supply documentation to the IAO stating patch numbers applied and the purpose of the patches.

- SAs did not apply the latest operating system or security-related service packs to 10 of 54 Windows servers. Windows 2000 STIG (SDID 2.005) requires the IAO to ensure that the latest operating system service packs are applied and documented. Windows 2003 STIG (SDID 2.019) requires that security-related software patches be applied.

An SA for a UNIX device indicated that the device did not have the latest security patches installed because their customer must approve all patches before installing them on the device. As a result, some tested systems did not have current releases of the required operating system.

SAs stated they rely on the FSO to identify what patches should be applied to systems. SAs also indicated that they could not receive patches from a vendor site without the patches undergoing testing and being approved through the Information Assurance Vulnerability Alert process. However, the FSO does not test any of the vendor-released patches, and the site SAs have the responsibility to test the vendor-released security patches. A Windows System Update Service server located in the Montgomery Systems Management Center offered a government sponsored automated patching tool from which the SAs could securely obtain and apply vendor-released patches. The FSO also recommended the use of patching tools from Sun to update Sun UNIX devices. The information provided by the SAs and FSO point to a lack of clear guidance on the responsible party for researching, identifying, and testing patches.

Recommendation F.

F.1. We recommend that the Director, Center for Computing Services, develop a process to ensure that system administrators understand their specific roles for patch compliance. This process should include, at a minimum, the following items:

F.1.a. Document the specific Security Technical Implementation Guides related to patching that the administrators should follow to ensure compliance.

F.1.b. Clearly define and explain the patch process, who is responsible for researching what patches are applicable for a particular device, and who is responsible for testing the patches.

F.1.c. Provide guidance on using the automated patching tools for the various devices such as System Update Service server from Microsoft.

Management Comments. The Director concurred and stated that the SA Certification Program defines the SAs roles and responsibilities of systems patch compliance in accordance with the STIGs. The Director stated that it is the policy of CS to clearly define SA roles and responsibilities for each system and application in the Service Level Agreement signed by CS and the customer. Additionally, CS provides guidance on using automated patching tools for the various devices such as System Update Service server

from Microsoft. CS has a process in place to request extensions or exceptions of patch updates since the new patch may not be compatible with a certain application.

Audit Response. Although not addressed in the Director's response to this recommendation, CS would complete SA Certification for current SAs requiring further training by December 31, 2005. No further comments are required.

Finding G. System File Baselines. SAs had not fully implemented the system file baseline process on Windows and UNIX devices because licenses had expired on the toolset, Symantec's Enterprise Security Manager. If baseline comparisons are not conducted, system files could be altered or compromised without being detected resulting in the system running in a compromised state.

A baseline is a database that contains a snapshot of the system after it has been fully loaded with operating system files, applications, and users. Baseline control consists of comparing a current system snapshot with the original system snapshot. Maintaining and checking a system baseline detects unauthorized, undocumented system changes. Unauthorized changes may indicate system compromise and a baseline may prevent serious damage by detecting unauthorized changes in a timely manner.

- SAs did not establish baselines or conduct baseline reviews for 31 of 54 Windows devices. The Windows Checklist (SDID 1.024) requires the SA to conduct baseline reviews weekly on each critical system.

- For 7 of 49 UNIX devices, the SA did not use a baseline utility program or appropriate commands to look for unauthorized sgid[4] files and compare baselines at least weekly. The UNIX STIG **(**SDID G085) requires the SA to use a baseline utility program or the appropriate command, such as the find command, to look for unauthorized sgid files at least weekly.

DoD, under U.S Strategic Command leadership, is working to provide enterprise solutions for all systems to have a secure configuration by installing accurately configured systems, sustaining the secure configuration with a compliance checking tool, automating the remediation to return the system to the secure configuration and reporting to reflect the system's configuration. DoD developed the Secure Configuration Compliance Validation Initiative, an automated vulnerability assessment solution, to determine whether a particular device is configured properly. DoD also developed the Secure Configuration Remediation Initiative, tool to automate the remediation of devices to return the system to the secure configuration. System Support Office Montgomery also developed self-healing scripts to remediate devices.

Recommendation G.

G.1. We recommend that the Director, Center for Computing Services, disseminate and require the use of automated tools such as Secure Configuration Compliance Validation Initiative and Secure Configuration Remediation Initiative, along with self-healing scripts that provide baseline

[4] Set Group ID (sgid) files are crucial to the correct operation of the UNIX operating system. The user executing the file has the same privileges as the group owner of the file. Therefore, unauthorized sgid files present a security hazard.

capabilities and the ability to compare system files to stored baseline configurations.

Management Comments. The Director concurred and agreed to direct all sites to implement automated tools such as Secure Configuration Compliance Validation Initiative and Secure Configuration Remediation Initiative along with self-healing scripts that are being tested and furnished by the SSO-Montgomery. As of August 1, 2005, Retina is the approved scanning Secure Configuration Compliance Validation Initiative and Secure Configuration Remediation Initiative tool.

Finding H. Encryption. Unix Devices did not always use an approved communications encryption method to perform remote management and file transfers. Specifically, SAs did not implement a remote administration encryption protocol, SSH, passwords for privileged accounts were not encrypted during remote access, and an application, such as TCP_WRAPPERS that allows an administrator to monitor and filter user access to network services. As a result, the affected devices could introduce security weaknesses into the production environment. During data transmission, a malicious user could gain access to unauthorized information and create a security breach by obtaining valid user credentials from systems not using encryption, or using a weak form of encryption. Once user credentials have been obtained, the user could compromise the shared data on the system. Depending on the sensitivity of the data, this could lead to the compromise of the system, or potentially other systems.

Secure Shell Protocols. The SAs did not install the correct version of the SSH protocol or did not use the correct version compatibility on 30 of 49 UNIX devices. The UNIX STIG (SDID G513) did not allow use of SSH protocol version 1, or SSH protocol version 1 compatibility mode. UNIX STIG (SDID Z1249) requires installation of the latest vendor version of SSH. Systems that use the SSH protocol version 1 or are configured to have version 1 compatibility mode are subject to Man in the Middle attacks. A malicious user could intercept the data transfer between source and destination systems, capture this information, and retransmit the data. The source and destination systems would not be aware of the attack because the data still arrives at its destination.

Encryption of Privileged Passwords. Privileged account passwords were not encrypted when accessing the device remotely on 37 of 49 UNIX devices. The UNIX STIG (SDID G499) requires the IAO to enforce that neither the root password, nor the passwords of users with root capable accounts, be passed over a network in clear text form; and UNIX STIG (Section 3.3.1.1) requires enhanced identification and authentication with encryption for each system accessed remotely by a privileged user. Running remote management and file transfer services that do not use approved encryption methods could reveal the password to malicious users who are eavesdropping on the network.

TCP_WRAPPERS. SAs did not use the TCP_WRAPPERS program, or equivalent, to secure Transmission Control Protocol communications for 5 of 49 UNIX devices. The TCP_WRAPPERS program allows an administrator to monitor and filter user access to network services. The UNIX STIG (SDID G196) requires implementation of the TCP_WRAPPERS program, or an equivalent, on all UNIX hosts connected to a network. Systems not configured to use the TCP_WRAPPERS program allow direct communication between the client and the network service. The TCP_WRAPPERS

program provided an additional layer of access control because it filters traffic based on the client's host information.

The UNIX STIG requires encryption to be used and stated that TCP_WRAPPERS or equivalent product could be used. However, CS did not provide guidance on where to obtain encryption products and how to implement those products. As a result, a gap existed between information provided in the criteria and implemented products. This gap led to devices that do not use communications encryption for remote management and file transfers, or use an out of date protocol.

Recommendation H.

> **H.1. We recommend that the Director, Center for Computing Services, update encryption guidance to include how to implement approved communications encryption methods for remote management and file transfers.**

Management Comments. The Director concurred and stated that CS expects to complete a policy containing specific guidance on how to implement approved communication encryption methods for remote management and file transfers on October 31, 2005.

Finding I. Outdated Technologies. The VMS database reported the DISA CS asset population included 10 Cabletron (network devices) and 538 Windows NT devices. Our sample verified that at least 3 Cabletron and 6 Windows NT devices still operated in the production environment. Vendors no longer support Cabletron and Windows NT systems, and the Cabletron devices do not support the network STIG password requirements. The vendor stopped providing support, bug fixes, and security updates for Windows NT in December 2004, and FSO stopped updates to the STIGs for Windows NT. FSO published a white paper on the migration process off of Windows NT, and is developing additional guidance for other technologies that may be used to prepare for technologies that will not be supported by vendors.

Cabletron. All three Cabletron devices tested did not have a unique username and password for each user. The Network Infrastructure Checklist (SDID 1372) requires that each account be assigned a unique username and password. All three Cabletron devices did not run the required version of SNMP since the device did not support SNMP version 3. The Network STIG (SDID 1660) rated this exception at the highest vulnerability category.

Windows NT. The Windows NT, Windows 2000, Windows XP Addendum requires the IAO to apply all security related software patches (SDID 2.019). The vendor stopped issuing security updates in December 2004, which caused the technology in the CS environment to not have security updates since December 2004. Additionally, FSO no longer updates the Windows NT STIG requirements; therefore, CS may not secure the technologies to meet DoD requirements.

Recommendations I.

I.1. We recommend that the Director, Center for Computing Services, develop and implement a plan to migrate all Windows NT and Cabletron devices to a supported operating system.

Management Comments. The Director concurred and stated that all Windows NT servers were directed to be decommissioned and replaced at all sites by December 30, 2004. The Computing Services Server Line of Business has been directed to conduct an inventory at all sites to ensure that Windows NT Servers have been replaced. The six servers that were identified during the diagnostic testing period of the SAS 70 audit were decommissioned on September 30, 2005. The Cabletron devices identified will be replaced by January 31, 2006.

I.2 We recommend that the Director, Center for Computing Services, prepare for technologies that will not be supported by vendors by developing long term scheduling and customer funding plans to ensure that system migrations to supported technologies are implemented before technologies become unsupported by the vendor.

Management Comments. The Director concurred and stated that there is a process in place for replacing non-supported technologies. CS notifies customers of upcoming unsupported technology issues as soon as it is notified. Additionally, DoD releases messages through the Defense Message System to inform all DoD Subordinate Commands of systems and technologies that will no longer be supported due to outdated technology.

Appendix A. Scope and Methodology

Overview

The Federal Information Systems Control Audit Manual general control testing required detail technical analysis of selected security settings and configurations. General controls testing encompassed diagnostic testing, the testing of the technical controls implemented in the CS environment. We developed work programs based on the STIGs and DoD Instruction 8500.2. Diagnostic testing consisted of an analysis of data extracted by automated scripts and supplemented by interviews with site SAs. Due to the large number and variety of system devices managed by CS, a statistical sampling approach was employed to select the items to be tested. Upon completion of testing, we summarized exceptions following DISA criteria, and statistically projected the results to the CS environment. A description of the sampling approach can be found in Appendix B.

Scope

The scope of the audit included CS unclassified systems located in the continental of United States. CS has 16 computing centers; however, statistical sample only contained systems managed by 11 computing centers. We performed diagnostic testing from December 2004 through June 2005, in accordance with Generally Accepted Government Auditing Standards. We performed diagnostic testing at the following 11 computing centers: Chambersburg, Pennsylvania; Columbus, Ohio; Denver, Colorado; Jacksonville, Florida; Mechanicsburg, Pennsylvania; Montgomery, Alabama; Norfolk, Virginia; Oklahoma City, Oklahoma; Ogden, Utah; San Antonio, Texas; and St. Louis, Missouri.

In total, CS manages over 4,600 system assets, unclassified systems located in the continental of United States, including mainframes, servers, and network devices. DISA FSO provided a list of CS assets as of September 2004. The list of assets contained mainframe (IBM, Unisys, Tandem, Virtual Machine, and Virtual Memory System), client server, network, UNIX, and Windows devices.

Methodology

The process to complete the diagnostic testing included: 1) generating a statistical sample from DISA's VMS, which maintained a list of CS assets and 2) consolidating the criteria and developing the process to review the test results.

The following process was implemented to review the assets:

- Developed technical server diagnostic work programs for each type of device that addressed specific DISA STIG, DoDI 8500.2 criteria, and industry recommended practices;

- Provided custom UNIX server diagnostic testing scripts to the FSO for evaluation and approval prior to running the scripts on any devices managed by CS;

- Evaluated IBM OS/390 configuration settings against work programs from output generated by Computer Associate Examine analysis tool provided by the FSO;

- Coordinated testing with Information Assurance Managers and SAs and observed diagnostic scripts execution on each device that captured system configuration and permission settings of key system files;

- Interviewed SAs for UNIX, Windows, network devices, OS/390, Tandem, and UNISYS at Defense Enterprise Computing Centers Montgomery; Columbus; Ogden; Oklahoma; Mechanicsburg; Chambersburg; Denver; Jacksonville; Norfolk; San Antonio; and St. Louis; for manual review portion of the work programs; and

- Compared the configuration and permission settings and the results from automated scripts and interviews against the criteria; and documented the conditions found for each work program step.

We used the DISA MIAG to determine the pass or fail of a device. The MIAG defined a single Category I finding as an automatic failure. The MIAG provided a predefined minimum closure rate for Category II and Category III findings. Failure to meet the predefined minimum closure rate would define an asset as failing. The diagnostic testing only focused on Category I and Category II findings. Table 1 contains the minimum closure rate for Category II findings.

Table 1: Testing Criteria

Operating System	Category II Min. Closure Rate
Windows	90%
UNIX	85%
Tandem	90%
LPAR (Mainframe)	85%
UNISYS	80%
Network Devices (Client/Servers)	90%

Scope Limitations. We did not complete testing on the entire population of devices in the statistical sample because of the following limitations:

- Due to funding constraints, the DoD Office of Inspector General issued a work stop order before all of the analysis and testing was completed on sampled devices. We gathered data from all sample devices but only completed analysis and testing on approximately 72 percent of the devices.

- Due to timing constraints, testing was not completed on four OS/390 mainframe and four Virtual Machine mainframes located in Mechanicsburg, Pennsylvania.

Use of Computer-Processed Data. We did not rely on computer-processed data to perform this audit. Rather, we assessed the configuration settings and controls implemented on the devices tested that involved computer-extracted data such as user password settings and services running on a device.

Use of Technical Assistance. The Technical Assessment Division of the DoD Office of Inspector General reviewed test plans and audit results. Additionally, we received assistance from the Quantitative Methods Division of the DoD Office of Inspector General for development of the sampling process.

Government Accountability Office High-Risk Area. The Government Accountability Office identified several high-risk areas in DoD. This report provides coverage of the effective Management of Information Technology Investments high-risk area.

Prior Coverage. Prior audit coverage will be addressed in a separate report, Report on General and Application Controls at the Defense Information Systems Agency, Center for Computing Services.

Appendix B. Sampling Approach

Objective

One of the audit objectives was to determine whether DISA CS general controls were adequately designed and operating effectively. We selected a sample of assets, covering different technologies, to determine the level of compliance with DoD and DISA policies. We followed the Government Accountability Office (GAO) Financial Audit Manual (FAM) Section 450 to determine a sample size for diagnostic testing. We utilized the sampling strategy to: obtain an estimated upper limit for the rate of logical information systems controls at risk in the population within five percent precision at the 90 percent confidence level for comparison to the GAO FAM; and obtain an overall estimate of the number of logical information systems controls at risk.

Sampling Design

Sample Frame. The FSO provided an inventory of CS systems extracted from the VMS. The FSO provided an inventory list that contained 5,233 assets across all CS data centers. An FSO official stated that the inventory provided was approximately 90 to 95 percent accurate as of September 15, 2004. We modified the inventory list by eliminating non-applicable assets, Defense Enterprise Computing Centers Europe and Pacific assets, and non-CS assets. As a result, the sampling frame contained 4,649 assets. Table 2 shows the modified sampling frame in ten groups.

Sample Size. Having no prior experience, we assumed a conservative expected deviation rate of 33 percent (at most, one out of three systems tested will have control exceptions). At 90 percent confidence, the estimated sample size needed in order to obtain 5 percent precision is 228 items. We imposed a minimum number of 10 items per group. For groups with less than 10 items, we selected all of the items. This resulted in a total sample size of 257 items.

As a result of decommissioned assets, the original sample of 257 devices decreased to 209 devices available for testing. In order to maintain a sufficient sample size, we supplemented 51 items to the sample. In addition, we supplemented additional 17 items in case more assets become decommissioned during field testing. There were no additional systems available for testing for Group E. We selected supplemental assets using the same random seed as the original sample in order to preserve the original selection probabilities and the randomness of the sample, and adjusted the sample size by group with a total increase of 68 supplemental items for a total of 277 devices in the adjusted sample size. Supplemental sample systems were only to be tested if the original sample items were found to be decommissioned. Defense Business Management System (DBMS) was moved into its own group (Group J) to ensure its inclusion in the sample to support another DoD Office of Inspector General audit. Table 3 shows the original sample size, the sample available for testing, and the adjusted sample size by group.

Table 2: Sampling Frame by Group

Group	IT Architecture	Number of Items
A	Client Server	36
B	Mainframe – IBM	214
C	Tandem	4
D	Mainframe – UNISYS	50
E	Mainframe – VM[1]	7
F	Mainframe – VMS[2]	1
G	Network	672
H	UNIX	1,692
I	Windows	1,972
J	Mainframe (DBMS)	1
Total		**4,649**

Table 3: Original and Adjusted Sample Size, by Group

Group	IT Architecture	Original Sample	Original Sample Available for Testing	Adjusted Sample Size
A	Client Server	10	7	11
B	Mainframe - IBM	11	11	16
C	Tandem	4	4	4
D	Mainframe - UNISYS	10	8	16
E	Mainframe - VM[1]	7	5	5
F	Mainframe - VMS[2]	1	1	1
G	Network	33	29	34
H	UNIX	83	66	87
I	Windows	97	77	102
J	Mainframe (DBMS)	1	1	1
Total		**257**	**209**	**277**

[1] Virtual Machine
[2] Virtual Memory System

Sample Results

Testing Criteria. To determine the passing or failing of each device, we used the MIAG issued by the CS Headquarters. See Appendix A for details.

Not all of the original sample and supplemental systems were tested and verified. The interruption of the sequence stopped the randomness of the samples and lead to a reduced sample for testing and analysis. We only used those systems that were tested and verified in the order of selection for the statistical estimation. A potential of 343 systems were either tested and verified or were found to be decommissioned. Table 4 identifies the potential 343 systems, by group, used for the estimation. The potential 434 systems includes systems that were tested and validated not in the order as selected, decommissioned items that were identified in the sample frame but were not part of the sample or supplemental items, and two non-sample items that were tested and validated. For the estimation calculations, we treated decommissioned devices as non-failures. Including the decommissioned items in the denominator of the calculation of the proportion of failures produces a conservative estimate of the percentage of failures and eliminates the introduction of another random variant in the estimation.

Only those systems that were tested and verified in the order of selection were used for the statistical estimation. Items that were not tested and verified in the order of selection were no longer part of the random sequence, and we identified these items as self-representing items. Because of the interrupted sample sequence, strata B (Mainframe - IBM), E (Mainframe - VM), and I (Windows) had insufficient sample items for statistical estimation, as shown in Table 5. Therefore, we excluded these three stratums from the sample and the sample frame for statistical estimation, as shown in Table 6. As a result, we used 218 of the potential 343 sample items for the statistical estimation. Self-representing items were separated from the sample and sample frame and assigned a weight of 1.0 in the statistical estimation processing.

Table 4: All Tested and Verified, or Decommissioned Systems

Group	IT Architecture	Number of Items
A	Client Server	24
B	Mainframe – IBM	7
C	Tandem	4
D	Mainframe – UNISYS	15
E	Mainframe – VM[1]	4
F	Mainframe – VMS[2]	1
G	Network	79
H	UNIX	94
I	Windows	114
J	Mainframe (DBMS)	1
Total		**343**

[1] Virtual Machine
[2] Virtual Memory System

Result Interpretations

Excluding strata B, E, and I, the estimated percent of logical information systems controls failures is 38.46 percent. The percentage of failures only applies to the 2,456 frame, as shown in Table 6. The 90 percent upper confidence boundary is 56.04 percent. According to the GAO FAM Section 450, at 90 percent confidence, an upper confidence boundary at less than 5 percent indicates that the auditors can have high reliance on controls; an upper confidence boundary between 5 percent to 10 percent indicates that the auditors can have moderate reliance on controls; and an upper confidence boundary at greater than 10 percent indicates that the auditors can have little or no reliance on controls. Thus, the estimate and the upper confidence boundary exceed the upper tolerable limits according to GAO FAM Section 450. Based on the sample results, we concluded that the logical information systems controls are not operating as designed.

Table 5. Sample Frame Counts by Stratum

		Original Counts				Sample Results												
						All[5]				In Order[6]				Self Representing[7]				
Grouping	IT Architecture	Original Population[1]	Sample Frame[2]	Original Sample[3]	Supplemental Items[4]	Pass	Fail	Decom-missioned	Total	Pass	Fail	Decom-missioned	Total	Pass	Fail	Decom-missioned	Total	Estimation Weights[8]
A	Client Server	36	36	10	4	2	3	19	24	2	2	8	12	0	1	11	12	2 00
B	Mainframe IBM	215	214	11	5	3	3	1	7	1	0	0	1	2	3	1	6	208 00
C	Tandem	4	4	4	0	3	0	1	4	3	0	1	4	0	0	0	0	1 00
D	Mainframe UNISYS	50	50	10	8	7	0	8	15	7	0	8	15	0	0	0	0	3 33
E	Mainframe VM	7	7	7	0	0	0	4	4	0	0	0	0	0	0	4	4	N/A
F	Mainframe VMS	1	1	1	0	0	0	1	1	0	0	1	1	0	0	0	0	1 00
G	Network	683	672	33	5	21	6	52	79	21	6	11	38	0	0	41	41	16 61
H	UNIX	1,774	1,692	83	21	8	41	45	94	1	4	3	8	7	37	42	86	200 75
I	Windows	2,040	1,972	97	25	18	36	60	114	0	1	0	1	18	35	60	113	1,859 00
J[9]	Mainframe (DBMS)	0	1	1	0	1	0	0	1	1	0	0	1	0	0	0	0	1 00
K[10]	Unknown	423	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	N/A
Total		**5,233**	**4,649**	**257**	**68**	**63**	**89**	**191**	**343**	**36**	**13**	**32**	**81**	**27**	**76**	**159**	**262**	

[1] The original population includes the entire universe of CS assets

[2] The sample frame includes items within the original population that were available for sample selection

[3] The original sample includes items that were selected for testing

[4] Supplemental systems were selected to to have a sufficient number of systems for testing and to achieve the precision requirements of 5 percent precision at 90 percent confidence.

[5] Includes all items that were tested and validated, or found to be decommissioned.

[6] Includes only sample items that were tested and validated in the order as selected.

[7] Includes items that were tested and validated not in the order as selected, decommissioned items that were identified in the frame that were not part of the sample or supplemental items, and two non-sample items that were tested and validated.

[8] The estimation weight is the inverse of the achieved sampling fraction, and is based on only those sample items tested and validated in the order as selected. The self-representing items were excluded from the frame and sample in order to calculate the

[9] After excluding the 423 items from the original group J, one item from Group B was identified as Mainframe DBMS and remained in the sample frame for Group J (Mainframe, DBMS).

[10] These items were part of Group J (Unknown) in the original population and were excluded from the sample frame.

Table 6. Sample Frame Counts by Stratum used for Estimation (Excludes Groups B, E and I)

		Original Counts				Sample Results												
						All[1]				In Order[2]				Self Representing[3]				
Grouping	IT Architecture	Original Population	Sample Frame	Original Sample	Supplemental Items	Pass	Fail	Decom-missioned	Total	Pass	Fail	Decom-missioned	Total	Pass	Fail	Decom-missioned	Total	Estimation Weights[4]
A	Client Server	36	36	10	4	2	3	19	24	2	2	8	12	0	1	11	12	2 00
C	Mainframe Tandem	4	4	4	0	3	0	1	4	3	0	1	4	0	0	0	0	1 00
D	Mainframe UNISYS	50	50	10	8	7	0	8	15	7	0	8	15	0	0	0	0	3 33
F	Mainframe VMS	1	1	1	0	0	0	1	1	0	0	1	1	0	0	0	0	1 00
G	Network	683	672	33	5	21	6	52	79	21	6	11	38	0	0	41	41	16 61
H	UNIX	1,774	1,692	83	21	8	41	45	94	1	4	3	8	7	37	42	86	200 75
J[5]	Mainframe (DBMS)	0	1	1	0	1	0	0	1	1	0	0	1	0	0	0	0	1 00
K[6]	Unknown	423	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	N/A
Total		**2,971**	**2,456**	**142**	**38**	**42**	**50**	**126**	**218**	**35**	**12**	**32**	**79**	**7**	**38**	**94**	**139**	

[1] Includes all items that were tested and validated, or found to be decommissioned.

[2] Includes only sample items that were tested and validated in the order as selected.

[3] Includes items that were tested and validated not in the order as selected, decommissioned items that were identified in the frame that were not part of the sample or supplemental items, and two non-sample items that were tested and valid.

[4] The estimation weight is the inverse of the achieved sampling fraction, and is based on only those sample items tested and validated in the order as selected.

[5] After excluding the 423 items from the original group J, one item from Group B was identified as Mainframe DBMS and remained in the sample frame for Group J (Mainframe, DBMS).

[6] These items were part of Group J (Unknown) in the original population and were excluded from the sample frame.

Appendix C. Criteria

All devices selected from the sample used the following criteria to determine whether each individually passed or failed the guidance to operate in the CS environment:

"Mandatory Information Assurance Guidance policy letter, Director Policy Letter 05-1, May 1, 2005."

The devices selected from the sample were tested against DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003 and the respective criteria as follows:

IBM Mainframe

"OS/390 Security Technical Implementation Guide," Version 4, Release 1, August 2003, Volume 1 and Volume 2.

"OS/390 Logical Partition Security Technical Implementation Guide," Version 2, Release 1, July 2003.

"SRR Review Procedures, OS/390 RACF Checklist," Version 4, Release 1.3, February 2004.

"SRR Review Procedures, OS/390 ACF2 Checklist," Version 4, Release 1.3, February 2004.

"SRR Review Procedures, OS/390 TSS Checklist," Version 4, Release 1.3, February 2004.

"SRR Review Procedures, MVS Logical Partition (LPAR)," Version 2, Release 1.3, June 2004.

Tandem

"Tandem Security Technical Implementation Guide," Version 2, Release 1, June 2003.

"Tandem Security Checklist," Version 2, Release 1.1, September 2003

Unisys

"Unisys Security Technical Implementation Guide," Version 6, Release 1, July 2003.

"Unisys Security Readiness Review Checklist UNISYSADM," Version 6.1.2, October 2003.

Network

"Network Infrastructure Security Technical Implementation Guide," Version 5, Release 2, September 2003.

"Network Infrastructure Security Checklist," Version 5, Release 2.2, September 2004.

"Cisco IOS Router Checklist Procedure Guide," June 2004.

"Juniper JUNOS Router Checklist Procedure Guide," June 2004.

UNIX

"UNIX Security Technical Implementation Guide," Version 4, Release 4, September 2003.

"UNIX Security Checklist," Version 4, Release 4, November 2004.

Windows

"Windows NT Security Checklist," Version 4, Release 1.6, June 2004.

"Windows 2000 Security Checklist," Version 4, Release 1.8, December 2004.

"Windows Server 2003 Security Checklist," Version 4, Release 0.0, December 2004.

Appendix D. Glossary

Authorized Program Facility (APF)	A component of OS/390 that allows installations to specify programs permitted to use sensitive system functions.
Crontab (cron services)	The crontab command, found in Unix and Unix-like operating systems, is used to schedule commands to be executed periodically. It reads a series of commands from standard input and collects them into a file known also known as a "crontab" which is later read and whose instructions are carried out. Generally, crontab uses a daemon, crond, which runs constantly in the background and checks once a minute to see if any of the scheduled jobs need to be executed. If so, it executes them. These jobs are generally referred to as cron jobs.
Daemon	On UNIX, a program running in the background, usually providing some sort of service. Typical daemons are those that provide e-mail, printing, telnet, file transfer protocol, and web access.
File Transfer Protocol (FTP)	An Internet tool/software utility that allows you to transfer files between two computers that are connected to the Internet. Anonymous FTP allows you to connect to remote computers and to transfer publicly available computer files or programs.
Host-based Intrusion Detection System (HIDS)	A software that monitors a system or applications log files. Host-based intrusion detection system responds with an alarm or a countermeasure when a user attempts to gain access to unauthorized data, file, or services.
Hypertext Transfer Protocol (HTTP)	The client server TCP/IP protocol used on the World Wide Web for exchange of Hyper Text Markup Language (HTML) documents. The client initiates the request to be sent an HTML document. The server responds by sending an HTML document.
Information Assurance Vulnerability Alert	The method that DoD agencies used for several years for monitoring and tracking resolution of network vulnerabilities.

Logical Partition	The division of a computer's processors, memory and storage into multiple sets of resources so that each set of resources can operate independently with its own operating system instance and applications.
Registry Keys	A central hierarchical database used in Microsoft Windows used to store information necessary to configure the system for one or more users, applications and hardware devices. The Registry contains information that Windows continually references during operation.
Resource Access Control Facility	An IBM software product. It is a security system that provides access control and auditing functionality for the z/OS and z/VM operating systems.
Secure Shell (SSH)	Sometimes known as Secure Socket Shell, is a Unix-based command interface and protocol for securely accessing a remote computer. It is widely used by network administrators to control Web and other kinds of servers remotely. SSH is actually a suite of three utilities - slogin, SSH, and scp - that are secure versions of the earlier UNIX utilities, rlogin, rsh, and rcp. SSH commands are encrypted and secure in several ways. Both ends of the client server connection are authenticated using a digital certificate, and passwords are protected by being encrypted.
Simple Network Management Protocol (SNMP)	The network management protocol of choice for TCP/IP based intranets. Defines the method of obtaining information about network operating characteristics, change parameters for routers and gateways.
TCP_WRAPPER	An application that monitors and filters incoming requests for network services.
Telnet	A utility program and protocol that allows one to connect to another computer on a network. After providing a username and password to login to the remote computer, one can enter commands that will be executed as if entered directly from the remote computer's console.

Transmission Control Protocol (TCP)	A communications protocol that provides a reliable host-to-host protocol between hosts in packet-switched communications networks and in interconnected systems of such networks.
User File Creation Mode Mask (umask)	A function on POSIX environments which sets the default file system mode for newly created files of the current process. Umask takes an integer as argument which is interpreted by applying it with bitwise and to the full access mode 077.

Appendix E. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense (Comptroller)/Chief Financial Officer
    Deputy Chief Financial Officer
    Deputy Comptroller (Program/Budget)

Department of the Navy

Naval Inspector General
Auditor General, Department of the Navy

Department of the Air Force

Auditor General, Department of the Air Force

Combatant Commands

Commander, U.S. Joint Forces Command
    Inspector General, U.S. Joint Forces Command
Commander, U.S. Strategic Command

Other Defense Organizations

Director, Defense Finance and Accounting Service
Director, Defense Information Systems Agency

Non-Defense Federal Organization

Office of Management and Budget

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Homeland Security and Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member (cont'd)

House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Efficiency and Financial Management, Committee on Government Reform
House Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform
House Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, Committee on Government Reform

Defense Information Systems Agency, Center for Computing Services Comments

DEFENSE INFORMATION SYSTEMS AGENCY
P. O. Box 4502
ARLINGTON, VIRGINIA 22204-4502

IN REPLY REFER TO Center for Computing Services (GS4) OCT 17 2005

TO: DOD Inspector General

VIA: DISA Inspector General

FROM: GIG Combat Support, Center for Computing Services (GS4)

SUBJECT: Response to Diagnostic Testing at DISA Center for Computing Services Project# D2004FG-0191.002

In accordance with established guidelines, attached is Computing Services' response to the Diagnostic Testing Report, issued 26 August 2005.

1 Enclosure a/s

ALFRED J. RIVERA
Director
Center for Computing Services

CENTER FOR COMPUTING SERVICES RESPONSES TO AUDIT D2004FG-0191.002
Conducted by DOD-IG
26 August 2005 Report

Diagnostic Testing at the DISA Center for Computing Services

Condition: Permissions, Settings, and Services. (Finding # A)

Compliance of technical controls with DoD and CS requirements and guidance needed improvement. Permissions to limit access to devices, directories and files, and registry setting, were not in compliance with DoD and DISA policies. Configuration and security settings for network, UNIX, Windows, and mainframe devices, were not in compliance with DoD and DISA guidelines. Services running on devices, configured incorrectly or should have been disabled, were not in compliance with DoD and DISA guidelines.

A.1.a DoD IG recommends that the Director, Center for Computing Services, develop a program to familiarize the system administrators of their specific roles in determining compliance. This program should include:

Specific Security Technical Implementation Guide Short Description Identifiers that the system administrators must comply with.

Center for Computing Services Response: Concur. Center for Computing Services has a Systems Administrator Certification program in place that ensures Systems Administrators are instructed on the Security Technical Implementation Guide Identifiers. The Field Security Office, with concurrence from Computing Services, has developed a plan to take over the responsibility of the Systems Administrator Certification Program. CSD will complete S/A Certification for current Systems Administrators requiring further training by 31 December 2005. The Field Security Office has provided Computing Services with a copy of their S/A certification program plan, which also includes an implementation time line. The S/A certification will be completed by 31 December 2005 and the maintenance period will begin on 2 January 2006.

A.1.b DoD IG recommends that the Director, Center for Computing Services, develop a program to familiarize the system administrators of their specific roles in determining compliance. This program should include:

Specific guidance on how to manually test Security Technical Implementation Guide Short Description Identifiers not tested by the automated scripts.

Center for Computing Services Response: Concur. Center for Computing Services Systems Administrator Certification Program covers instructions on how to manually test Security Technical Implementation Guide Short Description Identifiers not tested by the automated scripts. CSD will complete S/A Certification for current Systems Administrators requiring further training by 31 December 2005.

A.2 DoD IG recommends that the Director, Center for Computing Services, require the implementation of the Joint System Administration (JSA) Checklist, May 25, 2005, or an

equivalent, that provides system administrators with a list of tasks to be performed to bring the devices they manage into compliance with the Windows, UNIX, Tandem, IBM (OS/390), and Network Security Technical Implementation Guides.

Center for Computing Services Response: Concur. The JSA checklist has been incorporated at all CSD sites to ensure compliance with all Operating Systems and Network Security Technical Implementation Guides.

A.3 DoD IG recommends that the Director, Center for Computing Services, enforce the compliance with the Security Technical Implementation Guides for access permission settings, configuration and security settings, and disabling of unnecessary services.

Center for Computing Services Response: Concur. All site Information Assurance Managers have been re-briefed on the Security Technical Implementation Guides requirements to include access permissions settings, configuration and security settings. CSD will complete S/A Certification for current Systems Administrators requiring further training by 31 December 2005.

Condition: Automated Scripts. (Finding # B)

The automated UNIX script did not accurately report STIG compliance exceptions. The SAs who managed the devices depended on the automated script to identify exceptions that are not in compliance with STIG requirements. Specifically, the script did not check for all daemons, which are services on a UNIX system, or verify that only authorized shells were listed in the /etc/shells file. When the automated scripts did not report that a particular security setting had not met STIG requirements, or when the automated scripts did not identify the condition as an exception, then the exception or deficiency would not be identified by the SA and the system would remain non-compliant.

B.3 DoD IG recommends that the Director, Center for Computing Services, develop manual procedures for items reported by the automated script as Open and Not Reviewed and enforce performance of these procedures by the system administrators.

Center for Computing Services Response: Concur. CSD requires manual checks of all items reported by the automated script as "open" or "not reviewed" and enforces compliance with manual procedures already in place. FSO is in the process of updating the SRR scripts and expects to complete the SRR scripts by CY 2006. The SSO is also in the process of developing a Gold Disk for UNIX operating systems that will correct this finding. While the ratios of servers to Systems Administrators, and the number of possible open findings per server that are not reported by the current automated scripts make compliance with this task very challenging, DISA Computing Services Defense-in- Depth approach to information assurance and systems security helps mitigate this risk.

Condition: Password Policies. (Finding # C)

Password configurations did not always comply with DoD and DISA guidelines. For example, some password lengths were shorter than the minimum requirement, and some password aging

(the length of time a password can be used) was longer than the maximum time period allowed. As a result, the SAs did not find and remove noncompliant passwords or passwords did not expire for an extended period of time.

C.1 DoD IG recommend that the Director, Center for Computing Services, enforce compliance with the Security Technical Implementation Guides and ensure that password cracking tools are run on a weekly basis.

Center for Computing Services Response: Concur. Computing Services runs password-cracking tools on a weekly basis on all systems. The SRR scripts also include check for default passwords and privileged user accounts with no password. DOD and DISA Password requirements are addressed as part of the S/A certification program. CSD will complete S/A Certification for current Systems Administrators requiring further training by 31 December 2005.

C.2 DoD IG recommends that the Director, Center for Computing Services, enforce Department of Defense policy that requires passwords to be set, at a minimum, with a case sensitive, 8-character mix of upper case letters, lower case letters, numbers, and special characters, including at least one of each, and that passwords are changed every 90 days.

Center for Computing Services Response: Concur. DOD and DISA Password requirements are addressed as part of the S/A certification program. CSD will complete S/A Certification for current Systems Administrators requiring further training by 31 December 2005.

C.3 DoD IG recommends that the Director, Center for Computing Services, identify all customer applications that do not comply with system level password required settings, assess the risk presented by each instance of non-compliance, and require changes to the application or operating system to modify them to comply with the password requirements where the risks presented are unacceptable.

Center for Computing Services Response: Concur. CSD will work with customers to implement changes to their applications that are needed to meet the minimum user name and password requirements. Local site Directors are working with the customers to engage their support and cooperation in enforcing compliance with their required password settings.

C.4 DoD IG recommends that the Director, Center for Computing Services, check for and confirm registry keys that pertain to reversible password encryption are set to Department of Defense and Defense Information Systems Agency guidelines.

Center for Computing Services Response: Concur. Computing Services checks for and confirms registry keys that pertain to reversible password encryption settings are set to comply with Department of Defense and Defense information Systems Agency at all sites/location. All Sites are in compliance as of 17 October 2005.

Condition: Account Maintenance. (Finding # D)

- SAs did not implement account maintenance practices and procedures correctly for all devices. Specifically:

- SAs did not disable or change default accounts and passwords.
- SAs did not disable or delete inactive user accounts on systems after a period of non-use.

D.1 DoD IG recommends that the Director, Center for Computing Services, enforce the disabling of default accounts.

Center for Computing Services Response: Concur. CSD will re-iterate to the Directors and Deputy Directors the DOD and DISA guidelines for enforcing the disabling of default accounts at all sites/locations during the 31 October – 4 November 2005 CSD Operations Conference.

D.2 DoD IG recommends that the Director, Center for Computing Services, enforce the disabling of user accounts after a period of non-use and deletion of inactive user accounts.

Center for Computing Services Response: Concur. DOD and DISA guidelines for enforcing the disabling of user accounts after a period of non-use and deletion of inactive accounts will be enforced at all sites/locations. Furthermore, all departing employee accounts are deleted or re-assigned with a new user account name and Password as part of the check out process. DOD and DISA Password requirements are addressed as part of the S/A certification program. CSD will complete S/A Certification for current Systems Administrators requiring further training by 31 December 2005.

Condition: Intrusion Detection. (Finding # E)

CS did not deploy host-based intrusion detection system (HIDS) software on 30 of 54 Windows servers. DoD Instruction 8500.2 required that HIDS be deployed for all major applications and for network management assets such as routers, switches, and domain name servers. In addition, the Windows STIG (SDID 1.025) required the Information Assurance Manager to ensure DoD servers use HIDS.

E.1 DoD IG recommends that the Director, Center for Computing Services, identify all assets without host-based intrusion detection systems and implement host-based intrusion detection system as required by Department of Defense and Defense Information Systems Agency policies.

FSO Response: Concur. The DOD IA Tools Work Group is in the midst of testing and selecting a host base intrusion detection system for a DOD enterprise license. Therefore it is not economically or operationally feasible for Computing Service to do a large purchase of HIDS at this time. FSO Recommends that CSD make the best use of the HIDS they have based on the following criteria.; Customer Request, MAC I or MAC II (where there are no performance problems noted).

Center for Computing Services Response: Concur. CSD agrees with FSO recommendation and will implement HIDS enterprise wide once DOD IA Work Group publishes guidance.

Condition: System Patches. (Finding # F)

SAs did not always implement critical updates and system software patches for UNIX and Windows systems, or did not document that the customer waived the requirement to patch the systems. SAs may have misunderstood who authorized updates and system software patches, and the patch installation process. Running devices not adequately patched could introduce vulnerabilities already widely known, and a malicious individual could exploit the vulnerability. A patch release mitigates vulnerabilities, and the patch documentation also describes the vulnerability. The devices without patches posed risks to the CS network environment. Patching devices mitigates a substantial number of known vulnerabilities.
- SAs did not apply required software patches to 44 of 49 UNIX devices. The UNIX STIG (SDID G033) required that the SA ensure required software patches are applied to all devices and supply documentation to the IAO stating patch numbers applied and the purpose of the patches.
- SAs did not apply the latest operating system or security-related service packs to 10 of 54 Windows servers. Windows 2000 STIG (SDID 2.005) required the IAO to ensure that the latest operating system service packs are applied and documented. Windows 2003 STIG (SDID 2.019) required that security related software patches be applied. An SA for a UNIX device indicated that the device did not have the latest security patches installed because their customer must approve all patches before installing them on the device. As a result, some tested systems did not have current releases of the required operating system. SAs stated they rely on the FSO to identify what patches should be applied to systems. SAs also indicated that they could not receive patches from a vendor site without the patches undergoing testing and being approved through the Information Assurance Vulnerability Alert process. However, the FSO does not test any of the vendor-released patches, and the site SAs have the responsibility to test the vendor-released security patches. A Windows System Update Service server located in the Montgomery Systems Management Center offered a government sponsored automated patching tool from which the SAs could securely obtain and apply vendor-released patches. The FSO also recommended the use of patching tools from Sun to update Sun UNIX devices. The information provided by the SAs and FSO point to a lack of clear guidance on the responsible party for researching, identifying, and testing patches.

F.1 DoD IG recommends that the Director, Center for Computing Services, develop a process to ensure that system administrators understand their specific roles for patch compliance. This process should include, at a minimum, the following items:

a) Document the specific Security Technical Implementation Guides related to patching that the administrators should follow to ensure compliance.

b) Clearly define and explain the patch process, who is responsible for researching what patches are applicable for a particular device, and who is responsible for testing the patches.

c) Provide guidance on using the automated patching tools for the various devices such as System Update Service server from Microsoft.

Center for Computing Services Response: Concur. The Systems Administrator Certification program clearly defines the Systems Administrators roles and responsibilities of systems patch compliance in accordance with the Security Technical Implementation Guides. CSD policy is to clearly define System Administrator roles and responsibilities for each system and application in the Service Level Agreement signed by CSD and the customer. CSD Provides guidance on using automated patching tools for the various devices such as System Update Service server from Microsoft. CSD manages in excess of 1400 applications, including some that run on operating systems that require testing before patches can be applied. CSD has a process in place to request extensions or exceptions of patch updates since the new patch may not be compatible with a certain application. Therefore, the use of automated tools to update operating systems may not always be relevant.

Condition: System File Baselines (Finding # G)

SAs had not fully implemented the system file baseline process on Windows and UNIX devices because licenses had expired on the toolset, Symantec's Enterprise Security Manager. If baseline comparisons are not conducted, system files could be altered or compromised without being detected resulting in the system running in a compromised state.

G.1 DoD IG recommends that the Director, Center for Computing Services, disseminate and require the use of automated tools such as Secure Configuration Compliance Validation Initiative and Secure Configuration Remediation Initiative, along with self-healing scripts that provide baseline capabilities and the ability to compare system files to stored baseline configurations.

Center for Computing Services Response: Concur. CSD will direct that all sites implement automated tools such as SCCVI and SCRI along with self-healing scripts that are being tested and furnished by SSO Montgomery, as directed/recommended by FSO. Retina is the approved scanning, SCCVI and SCRI tool as of 1 August 05.

Condition: Encryption (Finding # H)

Unix Devices did not always use an approved communications encryption method to perform remote management and file transfers. Specifically, SAs did not implement a remote administration encryption protocol, SSH, passwords for privileged accounts were not encrypted during remote access, and an application, such as TCP_WRAPPERS that allows an administrator to monitor and filter user access to network services. As a result, the affected devices could introduce security weaknesses into the production environment. During data transmission, a malicious user could gain access to unauthorized information and create a security breach by obtaining valid user credentials from systems not using encryption, or using a weak form of encryption. Once user credentials have been obtained, the user could compromise the shared data on the system. Depending on the sensitivity of the data, this could lead to the compromise of the system, or potentially other systems.

H.1 DoD IG recommends that the Director, Center for Computing Services, update encryption guidance to include how to implement approved communications encryption methods for remote management and file transfers.

Center for Computing Services Response: Concur. CSD is in the process of developing a policy that includes specific guidance on how to implement approved communication encryption methods for remote management and file transfers. Policy will include the use of encryption tools such as Virtual Private Network, Secure Socket Layer, Secure Shell, and Public Key. CSD expects to complete this policy by 31 October 2005.

Condition: Outdated Technologies (Finding # I)

The VMS database reported the DISA CS asset population included 10 Cabletron (network devices) and 538 Windows NT devices. Our sample verified that at least 3 Cabletron and 6 Windows NT devices still operated in the production environment. Vendors no longer support Cabletron and Windows NT systems, and the Cabletron devices do not support the network STIG password requirements. The vendor stopped providing support, bug fixes, and security updates for Windows NT in December 2004, and FSO stopped updates to the STIGs for Windows NT. FSO published a white paper on the migration process off of Windows NT, and is developing additional guidance for other technologies that may be used to prepare for technologies that will not be supported by vendors.

I.1 DoD IG recommends that the Director, Center for Computing Services, develop and implement a plan to migrate all Windows NT and Cabletron devices to a supported operating system.

Center for Computing Services Response: Concur. Computing Services directed that all Windows NT servers be decommissioned and replace at all sites by 30 December 2004. A plan was in place to replace or decommission Windows NT servers under the CSD maintenance program. Computing Services Server Line of Business (LOB) has been directed to conduct an inventory at all sites to ensure that Windows NT Servers have been replaced. The six servers identified during the diagnostic testing period of the SAS 70 audit were decommissioned on 30 September 05. The Cabletron devices identified will be replaced by 31 January 2006.

I.2 DoD IG recommends that the Director, Center for Computing Services, prepare for technologies that will not be supported by vendors by developing long term scheduling and customer funding plans to ensure that system migrations to supported technologies are implemented before technologies become unsupported by the vendor.

Center for Computing Services Response: Concur. The process of replacing non-supported technologies is in place. Customers are made aware of upcoming unsupported technology issues as soon as CSD is notified. DOD releases messages through the Defense Message System to inform all DOD Subordinate Commands of systems and technologies that will no longer be supported due to outdated technology.

Defense Information Systems Agency, Field Security Operations Comments

INTEROFFICE MEMORANDUM

TO: DISA Inspector General (IG)

FROM: DISA Field Security Operations (GO4)

DATE: 4 October 2005

SUBJECT: Responses to Diagnostic Testing at the Defense Information Systems Agency Center for Computing Services Project # D2004-D000FG-0191.002

In accordance with established guidelines, attached is DISA FSO's response to the Diagnostic Testing at the Defense Information Systems Agency Center for Computing Services, dated 26 August 2005.

(b) (6) [redacted]

Enclosure a/s

Copy To:
CSD

Final Report
Reference

Diagnostic Testing
at the
Defense Information Systems Agency Center for Computing Services
Project No. D2004-D000FG-0191.002
Dated August 26, 2005

Field Security Operations representatives reviewed the draft IG report for Project No. D2004-D000FG-0191.002. Our comments follow:

Finding B. Automated Scripts.

Recommendations B.

Revised

B.1. We recommends that the Chief, Field Security Operations review the current scripts to determine if the information collected from the scripts provide enough assurance on the compliance or non-compliance of the device with the Security Technical Implementation Guides for Windows and UNIX requirements.

FSO Response. Concur. However, this finding is directly related to UNIX and not Windows. FSO will update the UNIX scripts by first quarter CY2006 to accurately check for all possible daemons/services. Additionally, FSO has added a contract modification for BAE and the nCircle Vendor to add STIG compliance testing/policies to their scanning and reporting tools. The projected completion date is 31 Dec 06.

B.2. We recommend that the Chief, Field Security Operations change the default value for the automated scripts from "Not a Finding" to "Not Reviewed" or some indicator that the script did not fully execute the test for compliance.

FSO Response. Concur. The DOD IG did identify a problem with the UNIX scripts defaulting to "Not a Finding" when they should have been defaulting to "Not Reviewed." Due to the large volume of scripts and on-going priorities, script fix actions will be completed in phases. As each script is "touched" to make other changes, the corrective action will be applied throughout the script to resolve the problem. Approximately 10% of the scripts were corrected in July 05. Scripts are updated every two months. The next script update is scheduled for October 05. Projected completion for all affected UNIX scripts is April 06. Additionally, FSO has added a contract modification for BAE and the nCircle Vendor to add STIG compliance testing/policies to their scanning and reporting tools. The projected completion for these efforts will be competed by 31 Dec 06.

B.3. We recommend that the Director, Center for Computing Services, develop manual procedures for items reported by the automated script as "Open" and "Not Reviewed" and enforce performance of these procedures by the system administrators.

FSO Response: In support of CSD, and as part of the FSO on-site IA Review process, validation reviews will be conducted to ensure that the CSD Security Automation process

is maintaining full compliance with the published STIGs. Exceptions will be noted and passed to SSO Montgomery for review and, if appropriate, corrective action.

Team Members

The Defense Financial Auditing Service, in conjunction with contract auditors from PricewaterhouseCoopers and the Technical Assessment Division of the Department of Defense Office of Inspector General (DoD OIG), prepared this report. Personnel of the Quantitative Methods Division, DoD OIG, also contributed to the report.

Paul J. Granetto

(b) (6)